IJH LAW
Ignacio J. Hiraldo (State Bar No. 354826)
1100 Town & Country Road Suite 1250
Orange, CA 92868
E: ijhiraldo@ijhlaw.com
T: 657.200.1403
Attorneys for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ROSEMARY ORTIZ, individually and on behalf of all others similarly situated,

Plaintiff,

v.

COINBASE, INC.,

Defendant.

Case No. 4:25-cv-4235

CLASS ACTION

CLASS ACTION COMPLAINT FOR NEGLIGENCE

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Rosemary Ortiz brings this class action against Defendant Coinbase, Inc., and alleges as follows upon personal knowledge as to Plaintiff and Plaintiff's own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by Plaintiff's attorneys.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") of Plaintiff and the Class members, including, without limitation: names, dates of birth, home addresses, phone numbers, financial account information, and Social Security numbers.

2. In the course of its cryptocurrency exchange operations, Defendant is entrusted with an extensive amount of Plaintiff's and the Class members' PII.

3. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed non-delegable legal and equitable duties to Plaintiff and the Class members.

4. On or about May 2025, unauthorized third parties accessed Plaintiff's and the Class members' PII (the "Data Breach Incident").

5. The full extent of the types of sensitive personal information, the scope of the breach, and the root cause of the Data Breach Incident is all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

6. Plaintiff's and the Class members' PII that was acquired in the Data Breach Incident can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and the Class members face a lifetime risk of identity theft.

7. Plaintiff's and the Class members' PII was compromised due to Defendant's negligent acts and omissions and the failure to protect Plaintiff's and the Class members' PII.

8. Plaintiff and Class Members continue to be at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

9. Defendant disregarded the rights of Plaintiff and the Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure their PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data in its possession. As a result, the PII of Plaintiff and

Class Members was compromised through access to and exfiltration by an unknown and unauthorized third party.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised because of Defendant's failure to: (i) adequately protect their PII; (ii) warn of Defendant's inadequate information security practices; (iii) effectively oversee, supervise, and secure equipment and the database containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents; and (iv) adequately supervise and oversee its vendor with whom it shared Plaintiff's and the Class Members' PII.

11. Plaintiff and Class members have suffered actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach Incident; (d) invasion of privacy; (e) the emotional distress and anguish, stress, and annoyance of responding to, and resulting from, the Data Breach Incident; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' PII against theft and not allow access and misuse of their personal data by others; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII, and, at the very least, are entitled to nominal damages.

12. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

13. Plaintiff is, and at all times relevant hereto was, a citizen and resident of South Carolina.

14. Defendant is, and at all times relevant hereto was, a Delaware corporation with headquarters located in Oakland, California.

JURISDICTION AND VENUE

15. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a putative class action involving thousands of Class Members and because the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Moreover, Plaintiff, many absent Class Members, and Defendant are citizens of different states.

16. This Court has general personal jurisdiction over Defendant because Defendant is headquartered in this jurisdiction.

17. Venue is proper in this district under 28 U.S.C. §§ 1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district.

FACTS

18. At the time of the Data Breach Incident, Defendant maintained Plaintiff's and the Class members PII utilizing a database and software.

19. By obtaining, collecting, and storing Plaintiff's and Class members' PII, Defendant assumed non-delegable legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

20. Plaintiff and Class members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, to make only authorized disclosures of this information, and to ensure that any vendor with whom Defendant shared the information was properly supervised and had the proper procedures in place to protect their PII.

21. Defendant had a non-delegable duty to adopt reasonable measures to protect Plaintiff's and Class members' PII, including any PII Defendant shared with any of its vendors, from involuntary disclosure to third parties.

22. Prior to the Data Breach Incident, Defendant should have ensured that (i) Plaintiff's and the Class Members' PII was properly encrypted or tokenized, (ii) it deleted such PII that it no longer had reason to maintain, (iii) it eliminated the potential accessibility of the PII from its vendor that was not justified, and (iv) it otherwise reviewed and monitored the security of its vendor's network system that contained the PII.

23. Prior to the Data Breach Incident, on information and belief, Defendant did not (i) ensure that its vendor's systems were encrypted or tokenized, (ii) ensure the deletion of such PII that it and/or its vendor no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from its vendor that was not justified, and (iv) otherwise review and improve the security of its network system that contained the PII.

24. On or about May 2025, Defendant mailed Plaintiff and the Class members a form notice attempting to minimize the Data Breach Event, while admitting that sensitive PII had been compromised and stolen.

25. Contrary to the self-serving narrative in Defendant's form notice, Plaintiff's and Class members' unencrypted information may end up for sale on the dark web and/or fall into the hands of companies that will use the detailed PII for targeted marketing without the approval.

26. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and the Class members.

27. Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII, relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

28. Defendant could have prevented the Data Breach Incident by ensuring the proper security and encryption of Plaintiff's and Class members' PII, or Defendant could have destroyed the data in its possession, especially old data from former inquiries and/or customers that Defendant had no legal right or responsibility to retain.

29. Defendant's negligence in safeguarding Plaintiff's and the Class members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

30. Despite the prevalence of public announcements and knowledge of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the Class members from being compromised.

31. The PII of Plaintiff and the Class Members was stolen to engage in identity theft and/or to sell it to criminals who will purchase the PII for that purpose.

32. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

33. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiff's and the Class members' PII, including data in its vendor's possession, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including,

specifically, the significant costs that would be imposed on Plaintiff and the Class members as a result of a breach.

34. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

35. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, potentially amounting to millions of individuals' detailed and confidential personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

36. The injuries to Plaintiff and the Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Plaintiff's and the Class members' PII, including PII Defendant provided to its vendor.

37. Plaintiff has suffered and will continue to suffer a substantial risk of imminent identity, financial, fraud and theft; emotional anguish and distress resulting from the Data Breach Incident, including emotion stress and damages about the years of identity fraud Plaintiff faces; and increased time spent reviewing financial statements and credit reports to determine whether there has been fraudulent activity on any of his accounts.

38. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

PROPOSED CLASS

39. Plaintiff brings this lawsuit as a class action on behalf of herself individually and on behalf of all other similarly situated persons as a class action pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and 23(c)(5). The "Class" that Plaintiff seeks to represent is defined as:

> **All residents of the United States whose PII was compromised in the Data Breach.**

40. Defendant and its employees or agents are excluded from the Class.

NUMEROSITY

41. The Data Breach Incident has impacted several thousand individuals. The members of the Class, therefore, are so numerous that joinder of all members is impracticable.

42. Identification of the Class members is a matter capable of ministerial determination from Defendant's records.

COMMON QUESTIONS OF LAW AND FACT

43. There are numerous questions of law and fact common to the Class which predominate over any questions affecting only individual members of the Class. Among the questions of law and fact common to the Class are: [1] Whether and to what extent Defendant had a non-delegable duty to protect the PII Plaintiff and Class members, including PII Defendant shared with its vendor; [2] Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members; [3] When Defendant actually learned of the Data Incident; [4] Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been compromised; [4] Whether Defendant failed to implement and

maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach Incident; [5] Whether Defendant adequately addressed and supervised the vulnerabilities which permitted the Data Breach Incident to occur; [6] Whether Plaintiff and the Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct; [7] Whether Plaintiff and the Class members are entitled to restitution as a result of Defendant's wrongful conduct; and [8] Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach Incident.

44. The common questions in this case are capable of having common answers. Plaintiff and the Class members will have identical claims capable of being efficiently adjudicated and administered in this case.

TYPICALITY

45. Plaintiff's claims are typical of the claims of the Class members, as they are all based on the same factual and legal theories.

PROTECTING THE INTERESTS OF THE CLASS MEMBERS

46. Plaintiff is a representative who will fully and adequately assert and protect the interests of the Class and has retained competent counsel. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Class.

SUPERIORITY

47. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the claims of all members of the Class is economically unfeasible and procedurally impracticable. While the aggregate damages sustained by the Class are in the millions of dollars, the individual damages incurred by each member of the Class resulting from Defendant's wrongful conduct are too small to warrant the expense of individual

lawsuits. The likelihood of individual Class members prosecuting their own separate claims is remote, and, even if every member of the Class could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

48. The prosecution of separate actions by members of the Class would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendant. For example, one court might enjoin Defendant from performing the challenged acts, whereas another may not. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

49. Plaintiff incorporates paragraphs 1-48 above as if fully set forth herein.

50. Plaintiff bring this claim on behalf of herself and the Class.

51. Defendant collected, stored, used, shared, and benefited from the non-public PII of Plaintiff and Class Members.

52. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

53. By collecting, storing, and using Plaintiff's and Class Members' PII, Defendant owed a non-delegable duty to Plaintiff and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII.

54. Defendant owed a non-delegable duty to prevent the PII it received from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

55. Defendant was required to prevent foreseeable harm to Plaintiff and Class Members, and therefore had a non-delegable duty to take adequate and reasonable steps to safeguard their sensitive PII from unauthorized release or theft.

56. This duty included: (1) designing, maintaining, and testing data security systems, data storage architecture, and data security protocols to ensure Plaintiff's and Class Members' PII in its possession was adequately secured and protected; (2) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely and adequate manner; (3) timely acting on all warnings and alerts, including public information, regarding its security vulnerabilities and potential compromise of the PII of Plaintiff and Class Members; and (4) maintaining data security measurers consistent with industry standards and applicable federal and state laws and other requirements.

57. Defendant had a non-delegable common law duty to prevent foreseeable harm to Plaintiff and Class Members. The duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices of Defendant in its collection, storage, sharing, and use of PII from Plaintiff and Class Members.

58. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their PII because malicious actors routinely attempt to steal such information for use in nefarious purposes, but Defendant also knew or should have known that it was more likely than not Plaintiff and Class Members would be harmed as a result.

59. Defendant's non-delegable duties to ensure the adequate and reasonable security measures of also arose as a result of the special relationship that

existed between it, on the one hand, and Plaintiff and Class Members, on the other hand. This special relationship arose because Defendant collected, stored, and used the PII of Plaintiff and Class Members for the procurement and provision of services for Plaintiff and Class Members.

60. Defendant alone could have ensured that the security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

61. Additionally, the policy of preventing future harm weighs in favor of finding a special relationship between Defendant and Plaintiff and Class Members. If companies are not held accountable for failing to take adequate and reasonable security measures to protect the sensitive PII with which they are entrusted, they will not take the steps that are necessary to protect against future security breaches.

62. The injuries suffered by Plaintiff and Class Members were proximately and directly caused by Defendant's failure to follow reasonable, industry standard security measures to protect Plaintiff's and Class Members' PII.

63. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

64. If Defendant had implemented the requisite, industry standard security measures and exercised adequate and reasonable care, data thieves would not have been able to take the PII of Plaintiff and Class Members.

65. Defendant breached these duties through the conduct alleged herein by, including without limitation, failing to protect the PII; failing to supervise and ensure the maintenance of adequate computer systems and allowing unauthorized access to and exfiltration of Plaintiff's and Class Members' PII; failing to disclose the material fact that Defendant's computer systems and data security practices were inadequate

to safeguard the PII from theft; and failing to disclose in a timely and accurate manner to Plaintiff and Class Members the material fact of the Data Breach.

66. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

67. As a direct and proximate result of Defendant's failure to exercise adequate and reasonable care and use commercially adequate and reasonable security measures, the PII of Plaintiff and Class Members were accessed by ill-intentioned individuals who could and will use the information to commit identity or financial fraud.

68. Plaintiff and Class Members face the imminent, certainly impending, and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

69. There is a temporal and close causal connection between Defendant's failure to implement security and supervisory measures to protect the PII of current and former patients and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members.

70. It was foreseeable that Defendant's failure to exercise reasonable care to safeguard the PII in its possession or control would lead to one or more types of injury to Plaintiff and Class Members, and the Data Breach Incident was foreseeable given the known, high frequency of cyberattacks and data breaches in the financial industry.

71. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting, storing, and sharing PII, the critical importance of providing adequate security of PII, the current cyber scams being perpetrated on PII, and that it had inadequate protocols, including security protocols in place to secure the PII of Plaintiff and Class Members.

72. Defendant's own conduct created the foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included their failure to take the steps and opportunities to prevent the Data Breach and their failure to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

73. Plaintiff and Class Members have no ability to protect their PII that was and is in Defendant's possession. Defendant alone was and is in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach Incident.

74. As a direct and proximate result of Defendant's negligence as alleged above, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering: (a) the compromise, publication, theft and/or unauthorized use of their PII; (b) unauthorized use and misuse of their PII; (c) the loss of the opportunity to control how their PII are used; (d) out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud; (e) lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach Incident, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud; (f) the imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals; (g) the continued risk to their PII that is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in Defendant's possession; and (h) current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach Incident for the remainder of the lives of Plaintiff and Class Members; (i)

loss of privacy; and (j) emotional distress and anguish related to the years of potential identity theft they face.

75. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered, and continue to suffer, damages arising from the Data Breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for the following relief:

a) An order certifying this case as a class action on behalf of the Class as defined above, and appointing Plaintiff as the representative of the Class and Plaintiff's counsel as Class Counsel;

b) Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class members;

c) Injunctive relief, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order: (1) requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws; (2) requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy

interests of Plaintiff and Class Members; (3) requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff and Class Member's personal identifying information; (4) prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database; (5) requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors; (6) requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring; (7) requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; (8) requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems; (9) requiring Defendant to conduct regular database scanning and securing checks; (10) requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members; (11) requiring Defendant to routinely and continually conduct internal

training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (12) requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information; (13) requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated; (14) requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; (15) requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and (16) for a period of 10 years, appointing a qualified and independent third party assessor to conduct attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

d) For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

e) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f) For prejudgment interest on all amounts awarded; and

g) Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demand a trial by jury.

DATED: May 16, 2025

Respectfully submitted,

IJH LAW

By: */s/ Ignacio Hiraldo*
Ignacio J. Hiraldo (State Bar No. 354826)
1100 Town & Country Road Suite 1250
Orange, CA 92868
E: ijhiraldo@ijhlaw.com
T: 657.200.1403

HIRALDO P.A.
Manuel S. Hiraldo, Esq.
Florida Bar No. 030380
401 E. Las Olas Boulevard
Suite 1400
Ft. Lauderdale, Florida 33301
Email: mhiraldo@hiraldolaw.com
Telephone: 954.400.4713
Pro Hac Vice to be filed
Counsel for Plaintiff